DATE(S) ISSUED:
2/9/2011

SUBJECT:
Multiple Vulnerabilities in Adobe Flash Player

OVERVIEW:
Thirteen security vulnerabilities have been identified in Adobe Flash Player. Adobe Flash Player is a widely distributed multimedia and application player used to enhance the user experience when visiting web pages or reading email messages. These vulnerabilities can be exploited if a user visits a malicious website or opens an email containing Flash media designed to exploit these vulnerabilities. Successful exploitation of one of these vulnerabilities may result in an attacker gaining the same privileges as the logged on user. If the user is logged in with administrator privileges, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
- Adobe Flash Player 10.1.102.64 and earlier

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
Thirteen security vulnerabilities have been identified in Adobe Flash Player. These vulnerabilities can be exploited if a user visits a malicious website or opens an e-mail attachment containing a file designed to trigger these issues. The vulnerabilities are as follows:
- Ten memory corruption vulnerability that could lead to code execution
- One Integer overflow vulnerability that could lead to code execution
- One font parsing input validation vulnerability that could lead to code execution
- One DLL Loading vulnerability that could lead to code execution

Successful exploitation may result in an attacker gaining the same user privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:
- Apply the appropriate updates provided by Adobe immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users not to open e-mail attachments from unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Adobe:

http://www.adobe.com/support/security/bulletins/apsb11-02.html

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0608
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0607
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0561
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0578
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0574
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0572
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0573
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0571
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0560
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0559
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0558
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0577
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0575